BANYAN SECURITY

Zero Trust Network Access (ZTNA) Evaluation Checklist

Problem

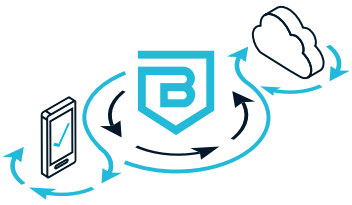
Providing secure remote access to infrastructure and applications at scale is challenging. Traditional network-centric solutions like VPNs have been put to the test and revealed significant performance, usability, and systemic security issues that band-aids cannot fix.

The workforce and talent acquisition is evolving. Post-COVID-19, a significant percentage of workers remain remote, and hiring is now best-in-class, not best-in-geographic-region. Increasing reliance on contractors, partners, and other contingent workers makes onboarding, offboarding, and BYOD support critical.

Infrastructures grow ever more complex, with applications spread across on-premises, hybrid, and multi-cloud environments.

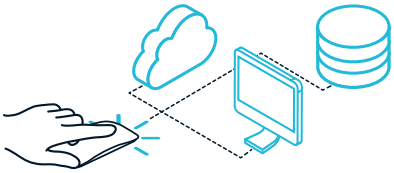
The remote access strategy that most companies have in place can't keep up with these realities. A scalable and comprehensive approach to secure remote access is required. Zero Trust Network Access should be evaluated as part of this new strategy.

Use Cases



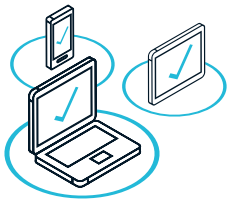
Replace Legacy VPN

Protect company resources by enabling least-privilege access to specific applications and servers based on real-time contextual factors including user and device trust scoring and resource sensitivity.



Provide Consistent, Easy Access for Engineering Teams

Provide user-friendly, VPN-free, least-privilege access to key DevOps infrastructure with one-click access to SSH/RDP and Kubernetes environments, including hosted applications like GitLab, Jenkins, and Jira.



Support BYOD and Third-Party Access

Enable a BYOD without needing Mobile Device Management (MDM) or Unified Endpoint Management (UEM) installed on each device. Corporate assets are continually protected while delivering an enhanced user experience that doesn't require control of their preferred devices.

Operational Changes

Before	After	Security Benefit
Network focus, access is granted based on the network where the desired resource resides.	Focus is on access to distributed assets spanning all environments and protocols, regardless of network or location.	Every network, resource, and asset can be configured for least-privilege access using the internet as transport with micro-tunnels securing the data.
Users can access all network resources once they authenticate to a network, unless there is network microsegmentation.	Use of microsegmentation for granular access control at the application, protocol, URL, or resource level without needing network segmentation.	Prevents lateral movement for a threat actor because access control is refined and granular, leaving little room to wander across a network and its resources.
Distributed security access control based on who owns the network, different approaches for on-premises, hybrid, and multi-cloud environments. Different approaches for employees, developers, and contractors.	Centralized access control and policy enforcement supporting any type of work by any person at any location.	Reduces attack surface risk, every resource and access is managed with the same process and controls regardless of what type of environment or business use.
Access policies are referenced a single time to initially authenticate users. Updates to policy may require end-user reboot or update to take effect.	Continuous re-authorization of users and devices against access policies. Policy updates are immediate and user access is dropped if privilege settings and device security are not met.	Policy adherence is constant rather than a snap-shot in time.
Some support for device security context with a mix of additional security tools and integrations.	Full device support, continuously verifying critical security elements and device certification, against access policies.	Minimize risk from device compromise when there is continuous revalidation of a device's security posture. This is especially important for access to sensitive and classified information.

Evaluation Checklist

Feature/Capability		BANYAN SECURITY	Vendor 1	Vendor 2
Installation	Immediate value – simple 15 min deployment	✔		
	100% software platform, no hardware or virtual appliance required	✔		
	Supports public and private cloud or on-premises installation	✔		
	Supports AWS CloudFormation templates for ease of deployment	✔		
	Purpose built cloud-native Zero Trust Network Access	✔		
	Requires minimal or no changes changes to corporate network infrastructure	✔		
Integration	Integrates easily with existing security tools	✔		
	IDaaS for authentication (e.g., Azure AD, Okta, Ping)	✔		
	MDM / EMM / UEM tools for device trust (ex. AirWatch, Intune, Jamf)	✔		
	EDR for real-time device health signals (e.g., Carbon Black, CrowdStrike, Sophos)	✔		
	Managed application configs for zero touch enrollment	✔		
	Export events/audit Logs to SIEMs (Splunk Phantom, Demisto, etc.)	✔		
Access Controls	Includes easy-to-use, human-readable policy engine for least privilege access controls	✔		
	Provides trust scoring framework that incorporates signals from existing tools as part of access and enforcement decisions	✔		
	Provides continuous device trust validation (context includes EDR running/OS version/firewall/encryption)	✔		
	Policy engine supports both managed devices and BYOD environments with ease	✔		
	Includes real-time event monitoring and alerting	✔		
	Provides continuous authorization via short-lived certificates and tokens	✔		
	Provides granular, API-level controls	✔		
	Provides user-to-application segmentation without providing access to the network	✔		
	Least privilege access restricts lateral movement	✔		
	Provides APIs for policy and config automation	✔		
Architecture	Cloaks applications from exposure to the public internet	✔		
	Provides an identity-aware proxy architecture designed for multi-cloud environments	✔		
	Provides a lightweight app installed on devices to continuously verify posture and establish device trust	✔		
	Flexibly supports cloud IaaS while also offering the option for enterprises to self-host their edge	✔		
	Integrates easily with existing IAMs through leading IAM marketplaces	✔		
	Incorporates native PKI for certs and integrates with existing PKI	✔		
Use Cases	Supports on-premises, hybrid- and multi-cloud, and SaaS use cases	✔		
	Hosted Web Applications – HTTP	✔		
	SaaS Applications – SAML/OIDC	✔		
	Servers – SSH/RDP, and Kubernetes	✔		
	Services – Database and other TCP	✔		
	Custom JSON	✔		

User Experience	Provides a unified services catalog for all of their services and web-apps	✔		
	Provides one-click access and autorun capabilities to infrastructure services	✔		
	Replaces user/password authentication to SSH with short-lived certificates	✔		
	Provides Zero Trust access that is transparent to end users	✔		
	Services can be grouped into bundles and users can add favorites for fast, easy access	✔		
	Frictionless access to use any SSH client and commands	✔		
	Supports passwordless zero trust access	✔		
	Includes option to expose trust score metrics to end users thereby decreasing support calls	✔		
	Trust score shown to end users to help improve their device security posture	✔		
	Provides easily customizable remediation descriptions and URLs enabling users to self-remediate	✔		
	Supports Windows/macOS/Linux/Android/iOS/iPadOS	✔		
Network	Requires minimal or no changes to existing networking infrastructure	✔		
	Roll out incrementally one service or application at a time	✔		
	No overlapping IP addresses and subnets to manage	✔		
	Uses cryptographic identity instead of IP address for network access	✔		
	No NGFW/VPN appliance required	✔		
	Requires minimal or no changes changes to corporate network infrastructure	✔		

About Banyan Security

Banyan Security provides zero trust network access to infrastructure and applications from anywhere on any device for employees, developers, and third parties without relying on network-centric solutions like VPNs. Leveraging its unique cybersecurity mesh architecture and trust scoring capabilities, Banyan provides passwordless, one-click access to complex infrastructure and applications. Risk and security are continuously evaluated and enforced in real-time across hybrid, multi-cloud, and SaaS environments. Banyan Security currently protects tens of thousands of employees across multiple industries, including finance, healthcare, manufacturing, and technology. To learn more, visit www.banyansecurity.io or follow us on Twitter at @BanyanSecurity.

BANYAN SECURITY

Banyan Security, Inc. | +1 415-289-9414 | www.banyansecurity.io